Comments from Privacy International and Access to the Review Group on Intelligence and Communications Technologies

October 4, 2013

Dear members of the Review Group on Intelligence and Communications Technologies:

Access - a 501(c)(3) organization committed to defending and extending the digital rights of people around the world - and Privacy International - a registered U.K. charity that was founded in 1990 and was the first organization to campaign at an international level on privacy issues - welcome the opportunity to submit for your consideration the *International Principles on the Application of Human Rights to Communications Surveillance* ("The 13 International Principles").

We are two of the 274 organizations from around the world that have endorsed the 13 International Principles, included below and available at https://en.necessaryandproportionate.org. The 13 International Principles can provide the Review Group with a framework to reassess and reform United States communication surveillance law in order to comply with its international human rights obligations. The 13 International Principles explain how existing international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. A well-crafted surveillance policy will archive the important objectives of protecting national security while upholding the United States' international human rights obligations.

We believe that the National Security Agency (NSA) has gone too far by bulk gathering content data under the FISA Amendments Act Section 702 and metadata under PATRIOT 215. Such mass surveillance fundamentally conflicts with the international obligations of the United States to protect and promote the right to privacy, enshrined in the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights. In drafting the Principles, advocacy organizations also considered laws like the Fourth Amendment to the U.S. Constitution's protection against unreasonable search and seizures, as well as U.S. Supreme Court cases like *United States v. Jones.*

At the core of the 13 International Principles is the recognition of the erosion of the distinction between communications data and content as a justifiable means of applying standards of legality, necessity, and proportionality. The 13 International Principles note,

> "While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may

> reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law."

The 13 International Principles are comprised of the following benchmarks against which, it is argued, communications surveillance laws must be measured to ensure they comply with international human rights standards:

- *Legality:* The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

- *Legitimate Aim:* Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

- *Necessity:* Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

- *Adequacy:* Any instance of communications surveillance authorised by law must be appropriate to fulfill the specific legitimate aim identified.

- *Proportionality:* Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and

expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy. Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. there is a high degree of probability that a serious crime has been or will be committed;
2. evidence of such a crime would be obtained by accessing the protected information sought;
3. other available less invasive investigative techniques have been exhausted;
4. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

1. other available less invasive investigative techniques have been considered;
2. information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3. information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

- *Competent Judicial Authority*: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:
    1. separate from the authorities conducting communications surveillance;
    2. conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and

3. have adequate resources in exercising the functions assigned to them.

- *Due Process:* Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

- *User Notification:* Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

    1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; and
    2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
    3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

- *Transparency:* States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

- *Public Oversight:* States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

- *Integrity of Communications and Systems:* In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.

- *Safeguards for International Cooperation:* In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

- *Safeguards Against Illegitimate Access:* States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these

principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

The 13 International Principles is a proposed framework in which the United States can evaluate whether current or proposed surveillance laws and practices are consistent with their human rights obligations. As the United States evaluates its practices, the 13 International Principles can be considered a roadmap for how fundamental rights can be met while addressing State's national security concerns. We urge the Review Group on Intelligence and Communications Technologies to assess whether the United States' surveillance practices meet its obligations under constitutional and international law.

Sincerely,

Carly Nyst
Head of International Advocacy
Privacy International

Fabiola Carrion
Policy Counsel
Access